



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification⁴ :

H04L 9/00

A1

(11) International Publication Number:

WO 88/02202

(43) International Publication Date: 24 March 1988 (24.03.88)

(21) International Application Number: PCT/US87/02301

(22) International Filing Date: 8 September 1987 (08.09.87)

(31) Priority Application Number: 905,775

(32) Priority Date: 10 September 1986 (10.09.86)

(33) Priority Country: US

(71) Applicants: M/A-COM GOVERNMENT SYSTEMS, INC. [US/US]; 3033 Science Park Road, San Diego, CA 92121 (US). CABLE/HOME COMMUNICATION CORP. [US/US]; 6262 Lusk Boulevard, San Diego, CA 92121 (US).

(72) Inventor: KATZNELSON, Ron, D.; 3913 Caminito Del Mar Surf, San Diego, CA 92130 (US).

(74) Agent: CALLAN, Edward, W.; 3033 Science Park Road, San Diego, CA 92121 (US).

(81) Designated States: AT (European patent), AU, BE (European patent), CH (European patent), DE (European patent), DK, FR (European patent), GB (European patent), IT (European patent), JP, LU (European patent), NL (European patent), NO, SE (European patent).

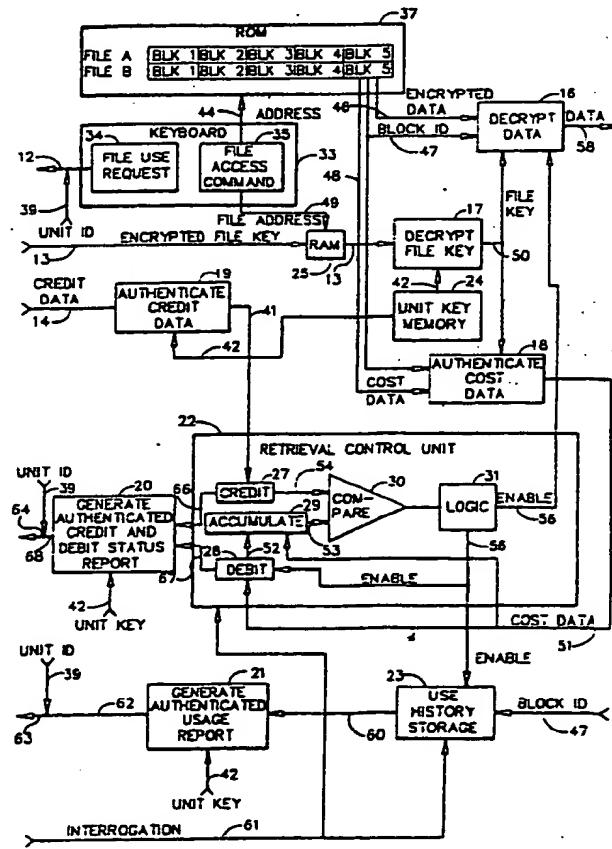
Published

With international search report.

(54) Title: METERING RETRIEVAL OF ENCRYPTED DATA STORED IN CUSTOMER DATA RETRIEVAL TERMINAL

(57) Abstract

A system for controlling and accounting for retrieval of data from a CD-ROM memory containing encrypted data files from which retrieval must be authorized. The system includes an authorization and key distribution terminal and a plurality of customer data retrieval terminals having such memories (37) loaded therein. The authorization terminal authorizes retrieval of data by authorized customer terminals by providing to the authorized customer terminals an encryption key (13) for enabling retrieval of the data and an authenticated credit signal (14) for use in limiting the amount of data to be retrieved from the files. The encryption key is encrypted for communication to the customer terminals in unique unit keys (42) that are stored (24) in the respective customer terminals. The customer terminal limits (22) the amount of data retrieved from the files in accordance with the credit signal; records (23) the amount of data retrieved from the files; and provides to the authorization terminal an authenticated report (62) of the recorded amount of data retrieved from said files. The memory (37) includes data files of different data vendors; and the customer terminal separately records (23) the retrieval of data from the files of the different vendors.



Best Available Copy

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT Austria	FR France	ML Mali
AU Australia	GA Gabon	MR Mauritania
BB Barbados	GB United Kingdom	MW Malawi
BE Belgium	HU Hungary	NL Netherlands
BG Bulgaria	IT Italy	NO Norway
BJ Benin	JP Japan	RO Romania
BR Brazil	KP Democratic People's Republic of Korea	SD Sudan
CF Central African Republic	KR Republic of Korea	SE Sweden
CG Congo	LI Liechtenstein	SN Senegal
CH Switzerland	LK Sri Lanka	SU Soviet Union
CM Cameroon	LU Luxembourg	TD Chad
DE Germany, Federal Republic of	MC Monaco	TG Togo
DK Denmark	MG Madagascar	US United States of America
FI Finland		

- 1 -

METERING RETRIEVAL OF ENCRYPTED DATA STORED IN CUSTOMER DATA RETRIEVAL TERMINAL

BACKGROUND OF THE INVENTION

The present invention generally pertains to data retrieval and is particularly directed to limiting and accounting for the retrieval of data from encrypted data files.

SUMMARY OF THE INVENTION

The present invention is a method and system for controlling and accounting for retrieval of data from a memory containing an encrypted data file from which retrieval must be authorized. The system includes means for authorizing such retrieval by providing an encryption key for enabling retrieval of the data and a credit signal for use in limiting the amount of data to be retrieved from the file; means for limiting the amount of data retrieved from the file in accordance with the credit signal; and means for recording the amount of data retrieved from the file. The system may further include means for reporting the recorded amount of data retrieved from the file; and means for authenticating such report.

The present invention is particularly suited for retrieving data files stored in a compact disc read-only-memory (CD-ROM).

-2-

Additional features of the invention are discussed in relation to the description of the preferred embodiment.

BRIEF DESCRIPTION OF THE DRAWING

Figure 1 is a block diagram illustrating the signals communicated between an authorization and key distribution terminal and a customer data retrieval terminal in a preferred embodiment of the present invention.

Figure 2 is a functional block diagram of the customer data retrieval terminal in the embodiment of Figure 1.

Figure 3 is a flow diagram showing operational routines in an alternative preferred embodiment of the present invention.

Figure 4 is a flow diagram showing operational routines in another alternative preferred embodiment of the present invention.

Figure 5 is a flow diagram showing certain aspects of the operational routines in still another alternative preferred embodiment of the present invention.

Figure 6 is a block diagram illustrating the use of a customer data retrieval terminal in a personal computer for retrieving data from a CD-ROM.

Figure 7 illustrates an exemplary scheme of tiering the retrieval of different types of data fields from a memory in accordance with a preferred embodiment of the present invention.

-3-

DESCRIPTION OF THE PREFERRED EMBODIMENTS

The use of a preferred embodiment of the system of the present invention is generally described with reference to Figure 1. The system essentially includes an authorization and key distribution terminal 10 and a customer data retrieval terminal 11; it being understood that in practice there are a plurality of customer data retrieval terminals 11 that communicate with a single authorization and key distribution terminal 10. A memory containing an encrypted data file from which retrieval must be authorized is loaded in the customer data retrieval terminal 11. different data files in the memory may be associated with different data vendors. Typically, communications between the authorization and key distribution terminal 10 and the customer data retrieval terminal 11 are transmitted over telephone lines.

In order to gain authorization to retrieve encrypted data from a given file stored in the memory loaded in the customer data retrieval terminal 11, the customer causes a file use request signal 12 to be communicated to the authorization and key distribution terminal 10. The file use request signal identifies the file for which retrieval authorization is requested and also contains an ID number identifying the customer terminal 11 from which the request signal 12 is sent.

-4-

The authorization and key distribution terminal 10 processes the request signal to determine whether the customer terminal 11 identified by the ID number contained in the file use request signal 12 is authorized to retrieve data from the file identified in the file use request signal 12. Such determination includes checking on the status of a customer account associated with the customer terminal 11 from which the request signal 12 is received; and may further include determining the eligibility of the customer to retrieve data from such file notwithstanding the outcome of the credit check.

Upon determining that the status of the customer account associated with the customer terminal 11 warrants authorizing retrieval of data from the file identified in the file use request signal 12, the authorization terminal 10 authorizes the customer terminal 11 to retrieve data from said file by providing to the customer terminal 11 both a file encryption key 13 and an authenticated credit data signal 14. The credit data signal 14 indicates an amount of credit to be extended to the customer terminal 11 for retrieval of data from the file identified in the file use request signal 12.

The file key 13 is encrypted in a unit key that is unique to the customer terminal 11 to which the encrypted file key 13 and the encrypted credit key 14 are being communicated. Unit keys for each of the customer terminals 11 associated with a given authorization and key distribution terminal 10 are stored in the authorization and key distribution terminal 10 and are individually retrieved in

-5-

accordance with the customer terminal ID number that is included in the file use request signal 12. Each customer data retrieval terminal also permanently stores its own unique unit key. The authenticated credit data signal 14 is generated by including both unencrypted credit data and encrypted credit data that is formed by encrypting the unencrypted credit data with the unit key of the customer terminal that is being authorized.

The operation of the customer data retrieval terminal 11 in retrieving the encrypted data from the memory loaded therein is described with reference to Figure 2. Certain functional units of the customer data retrieval terminal 11 are implemented in a microcomputer. These functional units include a data decryption unit 16, a file key decryption unit 17, a cost data authentication unit 18, a credit data authentication unit 19, an authenticated credit and debit status report generation unit 20, an authenticated usage report generation unit 21, a retrieval control unit 22 associated with each data vendor, a use history storage unit 23 associated with each data vendor, a unit key memory 24 and a random access memory (RAM) 25. The retrieval control unit 22 includes a credit register 27, a debit register 28, an accumulator 29, a comparator 30 and a logic unit 31. The customer data retrieval terminal 11 further includes a keyboard 33 for generating a file use request 34 and a file access command 35.

A read only memory (ROM) 37 containing the encrypted data files is loaded in the customer data retrieval terminal 11. The ROM 37 includes a plurality

-6-

of encrypted data files, File A, File B. Each data file includes encrypted data blocks, Block 1, Block 2, ..., Block 5. Each data file includes blocks of data of a given type of association. The different data files may be associated with different data vendors and there may be a plurality of data files associated with each of the different vendors. Each block of data includes encrypted data, a block ID (identification) signal, and authenticated cost data. The authenticated cost data indicates the cost associated with retrieving the given encrypted block of data.

To enable the customer data retrieval terminal 11 to retrieve data from any given file in the ROM 37, the file use request 34 identifying a given file is generated by use of the keyboard 33 and combined with the unit ID number 39 for the customer terminal 11 to provide the file use request signal 12 that is communicated to the authorization and key distribution terminal 10. As discussed above, the authorization and key distribution terminal 10 responds to the file use request signal 10 by providing the encrypted file key 13 and the authenticated credit data signal 14 to the customer terminal 11 when the authorization and key distribution terminal determines that the customer terminal 11 is authorized to retrieve the data identified in the file use request signal 12.

The encrypted file key 13 is stored in the RAM 25.

The received credit data signal 14 containing the credit data in both encrypted and unencrypted form is authenticated by the credit data authentication unit 19, which is keyed by the unit key 42 stored in the unit key memory 24 to

-7-

decrypt the encrypted credit data and thereby provide a decrypted credit data signal, which is compared with the unencrypted credit data signal in the authenticated credit data signal 14 to authenticate the received credit data signal 14. An authenticated credit data signal 41 is stored in the credit register 27 of the retrieval control unit 22 associated with the same vendor as the file from which data retrieval is being authorized. If the credit register 27 already has a credit balance, such balance is incremented by the amount indicated by the authenticated credit signal 41.

A message (not shown) indicating that authorization has been granted for the customer terminal 11 to retrieve data from the requested file is also communicated by the authorization and key distribution center 10 to the customer terminal 11 and displayed on a monitor (not shown) at the customer terminal 11.

To retrieve a given block of data from an authorized data file in the ROM 37, the keyboard 33 is operated to provide a file access command 35 which includes an address signal 44 directed to the ROM 37 for accessing the given block of data. In the example shown in Figure 1, the accessed block of data is block 5 of file B. Upon the block of data being accessed, the encrypted data 46, the block ID signal 47 and authenticated cost data 48 are read therefrom. The authenticated cost data includes both unencrypted cost data and encrypted cost data formed by encrypting the unencrypted cost data with the applicable file key for the file containing the block of data that is being retrieved.

-8-

The applicable encrypted file key 13 is retrieved from the RAM 25 in response to a file address 49 included in the file access command 35 and decrypted by the file key decryption unit 17, which is keyed by the unit key 42 stored in the unit key memory 24. The file key decryption unit 17 provides a decrypted file key 50 to the data decryption unit 16 and the cost data authentication unit 18.

The retrieved cost data signal 48 containing cost data in both encrypted and unencrypted form is authenticated by the cost data authentication unit 18, which is keyed by the file key 50 and initialized by the block ID signal 47 (used as an initialization vector) to decrypt the encrypted credit data and thereby provide a decrypted cost data signal, which is compared with the unencrypted cost data signal in the retrieved cost data signal 48 to authenticate the cost data signal.

An authenticated cost data 51 signal is provided to the debit register 28 and the accumulator 29. The debit register 28 is not immediately incremented by the cost data 51 signal, however. First the accumulator 29 adds the cost data signal 51 to a debit signal 52. The debit signal 52 indicates the sum of previous data retrieval costs accumulated in the debit register 28. The sum 53 of the cost data and the previously accumulated data retrieval costs indicated in the accumulator 29 is then compared by the comparator 31 with an accumulated credit signal 54 from the credit register 27 to determine whether the customer terminal 11 has been credited with sufficient credit to authorize retrieval of data from the

-9-

requested file. When the comparison indicates that there is sufficient accumulated credit to authorize such retrieval, the logic unit 31 provides an enable signal 56 to the data decryption unit 16, the debit register 28 and the use history storage unit 23. The enable signal 56 enables the cost data 51 to be incremented into the debit register 28. As noted above, the customer terminal 11 includes a plurality of retrieval control units 22 corresponding to a plurality of different vendors for accounting for the retrieval of data from the files associated with each of the different vendors.

The enable signal 56 also enables the operation of the data decryption unit 16. The data decryption unit 16 is keyed by the unit key 42 stored in the unit key memory 24 for decrypting the encrypted data 46 and providing retrieved data 58. The block ID signal 47 is used as an initialization vector by the data decryption unit 16 in combination with decrypted file key 50 for decrypting the decrypted data 46.

Upon being enabled by the enable signal 56, the use history storage unit 23 stores the block ID signal 47 to record the identity of the block of data retrieved from the ROM 37. The block ID signal identifies the file from which the data was retrieved and includes an address identifying the vendor associated with the retrieved file for addressing the use history storage unit 23 associated with the vendor of the data in the retrieved file. As noted above, the customer terminal 11 includes a plurality of use history storage units 23 corresponding to a plurality of

-10-

different vendors for separately recording the amount of data retrieved from the files associated with each of the different vendors.

5

A usage report 60 indicating the usage history recorded in the usage history storage unit 23 is generated for communication to the authorization and key distribution terminal 10 in response to either operation of the keyboard 33 or an interrogation signal 61 received from the authorization and key distribution terminal 10.

10

The block ID number further identifies the retrieved data by type; whereupon the type of data retrieved is recorded in the history storage unit 23 and included in the usage report 60.

15

An authenticated usage report 62 is generated by the authenticated usage report generation unit 21, which is keyed by the unit key 42 stored in the unit key memory 24, to encrypt the usage report. The authenticated usage report generation unit 21 provides the authenticated usage report 62, which includes the usage report in both encrypted and unencrypted form and is combined with the unit ID number 39 for communication to the authorization and key distribution terminal 10 as an authenticated usage report and unit ID signal 63.

20

Together with the authenticated usage report and unit ID signal 63, there also is communicated to the authorization and key distribution terminal 10 an authenticated credit and debit status report and unit ID signal 64. This signal 64 is provided in response to either operation of the keyboard 33 or the interrogation

- 11 -

signal 61 being directed to the retrieval control unit 22. Signals 66 and 67 respectively indicating the status of the credit and debit registers 27 and 28 are encrypted by the authenticated credit and debit status report generation unit 20, which is keyed by the unit key 42 stored in the unit key memory 24. The 5 authenticated credit and debit status report generator 20 provides an authenticated credit and debit status report signal 68, which includes such status report in both encrypted and unencrypted form, and which is combined with the unit ID number 39 to provide the authenticated credit and debit status report and unit ID signal 64.

The credit register 27, the debit register 28 and the use history storage 10 unit 23 for any given vendor can be reset to zero when desired in response to a refresh registers command 70 (Fig. 1) communicated from the authorization and key distribution terminal 10. Such command 70 would be communicated, for example, when a given customer terminal account associated with a given vendor is closed out.

15 In an alternative preferred embodiment, as shown in Figure 3, a separate file use request is communicated from a customer data retrieval terminal 72 to an authorization and key distribution terminal 73 for each data file that is to be retrieved. The operational routines illustrated in Figure 3 are implemented by a microcomputer.

20 Initially, a routine 75 is performed in the customer terminal 72 for generating an authenticated file use request containing a unit ID number 76 for the

-12-

customer terminal 72 and the file number 77 for the desired file. The generated file use request is encrypted in the unit encryption key 78 that is unique to the customer terminal 72 and communicated to the authorization and key distribution terminal 73 in an authenticated file use request message 79 that also includes the unencrypted unit ID number 76.

Upon receipt of the message 79, the authorization and key distribution terminal 73 performs a look-up routine 80 for looking up the unit key for the customer terminal 72 identified by the received unencrypted unit ID number.

Using the looked-up unit key 81, the authorization and key distribution terminal 73 performs a decryption routine 82 for decrypting the unit ID number and the desired file ID number from the received message 79.

The terminal 73 then performs another look-up routine 83, wherein the decrypted file ID number 84 is used to look up the file key 85 that was used for encrypting the file identified by the decrypted file number 84.

The terminal 73 also performs an authentication routine 86 for determining whether the received message 79 is authentic, wherein the decrypted unit ID number 87 is compared with the unit ID number contained in the received message 79. If it is determined from such comparison 86 that the message 79 is not authentic, the terminal 73 generates an error message 88 indicating that the received message 89 is not authentic. The error message is then communicated to and displayed 89 at the customer terminal 72.

- 13 -

If it is determined from the comparison 86 that the message 79 is authentic, the terminal 73 performs a credit check routine 90 for the customer terminal 72 identified by the unit ID number. If it is determined from such credit check 90, that credit should not be extended for retrieval of data from the requested file by the identified customer terminal 72, the authorization and key distribution terminal 73 generates an error message 88 indicating that credit is not authorized and communicates the error message to the customer terminal for display 89 at the customer terminal 72.

If it is determined from the credit check 90 that credit should be extended for retrieval of data from the requested file by the identified customer terminal 72, the file key 85 is encrypted in the unit key 81 for the identified customer terminal 72 by an encryption routine 91 and the encrypted file key 92 is communicated to the customer terminal 72.

The customer terminal 72 than performs a decryption routine 93, wherein the unit key 78 stored therein is used to decrypt the encrypted file key 92.

Next, the customer terminal performs a decryption routine 94, wherin the decrypted file key 95 is used to decrypt the file header for the encrypted data file 96 identified by the desired file number 77. The decrypted file header 97 is communicated to the authorization and key distribution terminal 73, which in turn performs a comparison routine 98 to determine whether the decrypted header is the correct header for the file identified by the decrypted file number 84. This

-14-

routine 98 verifies the decryption of the encrypted file key 92 communicated to the customer terminal 72 prior to debiting the account maintained for the customer terminal 72. If it is determined that the correct header has not been decrypted, the terminal 73 performs an error message routine 88, wherein an error message indicating the error is generated and communicated to the customer terminal 72 for display 89.

If it is determined that the correct header has been decrypted, an enable signal is communicated to the customer terminal 72 to enable a data file decryption routine 100. The enable signal 99 also initiates a routine 101 in the authorization and key distribution terminal 73, wherein a transaction report identifying the customer terminal 72 and the data file is generated and communicated to a billing terminal 102 for billing the customer associated with the customer terminal 72 for the retrieval of data from the requested file.

In an alternative preferred embodiment shown in Figure 4, an authorization terminal 105 and a customer terminal 106 perform several authentication and reporting routines. The operational routines illustrated in Figure 4 are implemented by a microcomputer.

Initially, the customer terminal 106 performs a routine 107 wherein an authorization request 108 containing the customer terminal unit ID number 109 is generated and communicated to the authorization terminal 105. The authorization terminal 105 performs a look-up routine 109 for looking up the unit key 110 for

-15-

the customer terminal 106 identified by the unit ID number contained in the request 108.

The authorization terminal then performs an authenticated signal generation routine 111, wherein the unit key 110 is used to encrypt an interrogation command. The encrypted interrogation command 112 is combined with the unencrypted interrogation command to provide an authenticated interrogation command, which is communicated to the customer terminal 106, where it is authenticated by using the unit key 113 stored therein.

The routines for generating authenticated given data that are described herein include the steps of encrypting the given data and generating a signal that includes the given data in both encrypted and unencrypted form.

The routines for authenticating given data that are described herein include the steps of decrypting given data that has been encrypted and comparing the decrypted data to the given data in unencrypted form.

It is to be understood that other techniques of generating authenticated data and of authenticating given data may be used in other embodiments of the present invention.

The customer terminal 106 responds to the interrogation command 112 by retrieving a use history report 114 for the user terminal 106 from a use history storage unit 115 and a debit and credit report 116 for the customer terminal 106

- 16 -

5

from debit and credit registers 117. The customer terminal then performs an authentication routine 118, wherein the unit key 113 is used to encrypt the use history report 114 and the debit and credit report 116. An authenticated report 119 including the reports 114 and 116 in both encrypted and unencrypted form is communicated to the authorization terminal 105.

10

The authorization terminal performs a routine 121 using the unit key 110 to authenticate the report 119. The use history and debit and credit reports also are processed in relation to each other in accordance with certain criteria to determine their authenticity. If it is determined that the reports 119 is not authentic, a report 123 is generated in the authorization terminal 105 and an error message is communicated to and displayed 124 in customer terminal 106.

15

If it is determined that the reports 119 is authentic, the use history is stored 125 for a report 125a to a billing terminal 126 and the authorization terminal 105 performs a credit check routine 127 in view of the status of the accounts for the customer terminal 106, as updated by the authenticated report 119, to determine whether the customer terminal 106 should be authorized to retrieve data from encrypted data files loaded therein. In conducting such credit check, the credit check routine 127 also accesses a credit look-up table 128 that includes a bad credit list 129 received from the billing terminal 126.

20

If the credit check routine 127 determines that the customer terminal 106 should not be authorized to retrieve data from encrypted data files loaded therein,

- 17 -

an error report 130 is generated in the authorization terminal 105 and an error message is communicated to and displayed 124 in the customer terminal 106.

If the credit check routine 127 determines that the customer terminal 106 should be authorized to retrieve data from encrypted data files loaded therein, the 5 authorization terminal 105 performs a routine 132, wherein the unit key 110 is used to generate an authenticated credit data signal 133, which is communicated to the customer terminal 106. The credit data signal indicates a predetermined number of retrieval units in accordance with the credit rating assigned to the customer terminal 106.

10 The customer terminal performs an authentication routine 134 on the credit data signal 133 by using the unit key 113 stored in the customer terminal 106. If it is determined pursuant to the authentication routine 134 that the credit data signal 133 is not authentic, an error message is displayed 124 in the customer terminal 106 and reported in the authorization terminal 105.

15 If the authentication routine 134 determines that the encrypted credit signal is authentic, the credit register in the customer terminal 106 is updated 136 and decryption of the data in the data file loaded in the customer terminal is enabled 137 in accordance with the amount of updated credit.

20 The operation of providing an encrypted file key from the authorization center 105 to the customer terminal 106 is not necessarily included in combination with the operations described in relation to the embodiment of Figure 4, although

- 18 -

it may be if desired. Alternatively, a file key for each vendor may be permanently stored in the customer terminal 106 for use in decrypting data encrypted in the file key for the respective vendor; or a file key for each vendor may be contained in a card that is independently loaded into the customer terminal 106, and which may be changed from time to time or in accordance with the particular vendor from whose data file the data is to be retrieved.

Figure 5 illustrates an exemplary series of operational routines that may be used with the embodiment of Figure 4 for controlling the retrieval of data from different encrypted data files associated with each vendor and for recording the retrieval of data from such files. The operations described with reference to Figure 5 are performed by a microcomputer in the customer terminal. In this example, each data file includes a plurality of data blocks and data blocks of different types. Each different type of data block has its own unique cost data manifested in a specified amount of retrieval units R associated therewith.

Pursuant to a plurality of retrieval routines 140, a quantity of N blocks of a type having a retrieval cost R are retrieved from data files associated with vendor Y; whereupon the use history storage for vendor Y is updated 141 and the debit register for vendor Y is incremented by N times R retrieval units 142. A comparison routine 143 is performed each time the debit register is incremented to determine whether the amount in the debit register for vendor Y is equal to or exceeds the amount in the credit register for vendor Y. If not, further data retrieval

- 19 -

from the data files associated with vendor Y may continue. When the amount in the debit register equals or exceeds the amount in the credit register, decryption is disabled 144 and a message that retrieval is "unauthorized" is displayed 145 at the customer terminal.

5 The customer then knows that he must cause the customer terminal to generate another authorization request 108, as in the embodiment of Figure 4, in order to receive a further credit signal from the authorization terminal and thereby increment the credit register before further retrieval from the data files of vendor Y will be authorized.

10 In view of its storage capacity and ease of data retrieval, a CD-ROM is preferred as the storage medium for the data files to be retrieved in accordance with the present invention. Referring to Figure 6, a CD-ROM 148 is loaded into a CD-ROM drive 149, which is connected to a customer data retrieval terminal 150, such as that described with reference to Figure 2. The customer data retrieval terminal 150 is contained in a microcomputer in a personal computer 151 and uses the microcomputer bus 152 to communicate with an authorization and key distribution terminal (not shown) via a telephone modem 153 and the telephone line 154.

15 The Data Encryption Standard (DES) algorithm is preferred for the encryption and decryption steps described herein. The unit key memory in the customer data retrieval terminals is a secure memory included in an integrated

-20-

circuit chip having an architecture that prevents the memory from being accessed from off the chip. The secure memory can be accessed only by the processor in the microcomputer that performs the DES algorithm.

5 The retrieval of different types of data from the memory loaded in the customer data retrieval terminal may be authorized in predetermined tiers corresponding to the different types of data, as shown in an example illustrated in Figure 7. In this example data file J includes data blocks 1, 2, 3, each of which include a plurality of corresponding different data fields a, b, c, d, e. Each of the commonly designated data fields is related to a common type of data. In the 10 example of Figure 7, each data block a, b, c, d, e, pertains to a different company; field "a" contains the company name; field "b" contains the zip code; field "c" contains the number of employees; field "d" contains the plant area; and field "e" contains annual revenue. Each data block also includes a block ID number.

15 In order to limit the retrieval authorization for different customer terminals to different types of data, the file key is subdivided into a plurality of field keys corresponding to the different data fields. Accordingly, the file key for data field J includes field keys a_J, b_J, c_J, d_J, e_J. Different authorization tiers A, B, C, are assigned to different customer terminals in accordance with the different combinations of the different types of data fields that they are authorized to retrieve. In the example of Figure 7, tier A is assigned to customer terminals authorized to retrieve data from all of the data fields in the data file; tier B is 20

-21-

assigned to customer terminals authorized to retrieve data from only fields b and d; and tier C is assigned to customer terminals authorized to retrieve data from only fields b, c, and e.

-22-

CLAIMS

1. A method of controlling and accounting for retrieval of data from a
2 memory, comprising the steps of

4 (a) providing a memory containing an encrypted data file from which
retrieval must be authorized;

6 (b) authorizing said retrieval by providing an encryption key for enabling
retrieval of said data and a credit signal for use in limiting the amount of data to
be retrieved from said file;

8 (c) limiting the amount of data retrieved from said file in accordance with
said credit signal; and

10 (d) recording the amount of data retrieved from said file.

2. A method according to Claim 1, further comprising the steps of

2 (e) reporting the recorded amount of data retrieved from said file; and

(f) authenticating said report.

3. A method according to Claim 1, wherein step (b) comprises the step

2 of

(g) encrypting said encryption key.

4. A method according to Claim 1, wherein step (b) comprises the step

2 of

-23-

(e) authenticating said credit signal.

5. A method according to Claim 1, further comprising the step of

2 (e) determining whether credit should be extended in response to a
retrieval request, and, if so, the amount of said credit to be indicated by said credit
4 signal.

6. A method according to Claim 1, wherein

2 step (a) comprises providing a memory containing encrypted data files for
each of a plurality of different data vendors, with a different said encryption key
4 being required to retrieve data file(s) associated with each of said vendors;

6 step (b) comprises providing a separate set of encryption key and credit
signal for each vendor associated with a said file retrieval authorization;

8 step (c) comprises limiting retrieval of files associated with different
vendors separately in accordance with the encryption key and credit signal
provided for said vendor; and

10 step (d) comprises separately recording the amount of retrieved data with
respect to each vendor.

7. A method according to Claim 6, wherein

2 step (a) comprises providing a memory containing a plurality of encrypted
data files for a given data vendor; and

-24-

4 **step (d) comprises separately recording the amount of retrieved data with respect to each data file of said given vendor.**

8. A method according to Claim 1, wherein

2 **step (a) comprises providing a memory containing a plurality of encrypted data files for a given data vendor; and**

4 **step (d) comprises separately recording the amount of retrieved data with respect to each data file of said given vendor.**

9. A method according to Claim 1, wherein

2 **step (a) comprises providing a said memory that further contains unencrypted initialization vector data associated with the encrypted data file; and**

4 **the method further comprises the step of**

6 **(e) using said initialization vector data in combination with said encryption key to retrieve data from said file.**

10. A method according to Claim 1, wherein

2 **step (a) comprises providing a said memory that further contains unencrypted initialization vector data uniquely associated with different blocks of data within the encrypted data file; and**

4 **the method further comprises the steps of**

6 **(e) using said initialization vector data in combination with said encryption key to retrieve data from said file; and**

-25-

8 (f) using said unique initialization vector data upon said retrieval to record
the identity of the block of data retrieved from said file.

11. A method according to Claim 1, wherein

2 step (a) comprises providing a said memory that further contains
unencrypted identification data uniquely associated with different blocks of data
4 within the encrypted data file; and

the method further comprises the step of

6 (e) using said unique identification data upon said retrieval to record the
identity of the block of data retrieved from said file.

12. A method according to Claim 1, wherein

2 step (a) comprises providing a said memory that further contains cost
data associated with different blocks of data that can be retrieved from said
4 memory; and

the method further comprises the steps of

6 (e) processing the cost data with said credit signal in response to a
request to retrieve a given said block of data to determine whether retrieval of
8 said requested block of data is authorized.

13. A method according to Claim 12, further comprising the step of

2 (f) authenticating said cost data prior to said processing of same.

-26-

14. A method according to Claim 1, wherein

2 **step (a) comprises providing said memory in a customer data retrieval terminal; and**

4 **step (b) comprises determining in an authorization center located remotely from said customer terminal whether the status of an account associated 6 with said customer terminal warrants authorizing said retrieval, and, if so, providing said encryption key and said credit signal in the customer data retrieval terminal.**

15. A method according to Claim 14, wherein

2 **step (a) comprises providing a said memory that further contains cost data associated with different blocks of data that can be retrieved from said 4 memory; and**

the method further comprises the steps of

6 **(e) recording in said customer terminal, the cost data for the blocks of data retrieved in relation to said credit signal provided therein; and**

8 **(f) reporting to the authorization center the record of said cost data in relation to said credit signal.**

16. A method according to Claim 15, further comprising the step of

2 **(g) authenticating said report of the record of said cost data in relation to said credit signal.**

-27-

17. A method of controlling and accounting for retrieval of data from a plurality of identical memories by a corresponding plurality of different data retrieval terminals, comprising the steps of

4 (a) providing a memory containing an encrypted data file from which retrieval must be authorized;

6 (b) providing a different unit key in each of the retrieval terminals;

8 (c) authorizing said retrieval by providing an encryption key encrypted in the unit key of the given retrieval terminal for enabling retrieval of said data in the given retrieval terminal and by providing a credit signal addressed to the given retrieval terminal for use in limiting the amount of data to be retrieved from said file by the given retrieval terminal;

12 (d) limiting the amount of data retrieved from said file in the given retrieval terminal in accordance with said credit signal; and

14 (e) recording the amount of data retrieved from said file in said retrieval terminal.

18. A method of controlling and accounting for retrieval of data from a memory in a customer data retrieval terminal, comprising the steps of

2 (a) providing in the customer data retrieval terminal a memory containing an encrypted data file from which retrieval must be authorized;

4 (b) authorizing said retrieval in response to a request to retrieve data

-28-

6 from said file in said customer data retrieval terminal by determining in an
8 authorization center located remotely from the customer terminal whether the
status of an account associated with said customer terminal warrants authorizing
10 said retrieval, and, if so, providing in the customer terminal an encryption key for
enabling retrieval of data from said file; and

12 (c) recording the retrieval of data from said file by said customer retrieval
terminal and debiting said account for said retrieval.

19. A method according to Claim 18, wherein step (b) comprises the step
2 of

(d) encrypting said encryption key.

20. A method according to Claim 18, further comprising the step of

2 (d) verifying decryption of data pursuant to use of said encryption key
prior to debiting said account.

21. A system for controlling and accounting for retrieval of data from a
2 memory containing an encrypted data file from which retrieval must be authorized,
comprising

4 means for authorizing said retrieval by providing an encryption key for
6 enabling retrieval of said data and a credit signal for use in limiting the amount of
data to be retrieved from said file;

8 means for limiting the amount of data retrieved from said file in
accordance with said credit signal; and

-29-

means for recording the amount of data retrieved from said file.

22. A system according to Claim 21, further comprising

means for reporting the recorded amount of data retrieved from said file;

and

4 means for authenticating said report.

23. A system according to Claim 21, wherein the authorization means

comprises

means for encrypting said encryption key.

24. A system according to Claim 21, wherein the authorization means

comprises

means for authenticating said credit signal.

25. A system according to Claim 21, further comprising

means for determining whether credit should be extended in response to
a retrieval request, and, if so, the amount of said credit to be indicated by said
4 credit signal.

26. A system according to Claim 21, wherein

said memory contains encrypted data files for each of a plurality of
different data vendors, with a different said encryption key being required to
4 retrieve data file(s) associated with each of said vendors;

-30-

6 the authorization means comprises means for providing a separate set of
encryption key and credit signal for each vendor associated with a said file
retrieval authorization;

8 the limiting means comprises means for limiting retrieval of files
associated with different vendors separately in accordance with the encryption key
10 and credit signal provided for said vendor; and

12 the recording means comprises means for separately recording the
amount of retrieved data with respect to each vendor.

27. A system according to Claim 26, wherein

2 the memory contains a plurality of encrypted data files for a given data
vendor; and

4 the recording means comprises means for separately recording the
amount of retrieved data with respect to each data file of said given vendor.

28. A system according to Claim 21, wherein

2 the memory contains a plurality of encrypted data files for a given data
vendor; and

4 the recording means comprises means for separately recording the
amount of retrieved data with respect to each data file of said given vendor.

29. A system according to Claim 21, wherein

-31-

2 the memory further contains unencrypted initialization vector data
associated with the encrypted data file; and

4 **the system further comprises**

6 means for using said initialization vector data in combination with said
encryption key to retrieve data from said file.

30. **A system according to Claim 21, wherein**

2 the memory further contains unencrypted initialization vector data
uniquely associated with different blocks of data within the encrypted data file; and

4 **the system further comprises**

6 means for using said initialization vector data in combination with said
encryption key to retrieve data from said file; and

8 means for using said unique initialization vector data upon said retrieval
to record the identity of the block of data retrieved from said file.

31. **A system according to Claim 21, wherein**

2 the memory further contains unencrypted identification data uniquely
associated with different blocks of data within the encrypted data file; and

4 **the system further comprises**

6 means for using said unique identification data upon said retrieval to
record the identity of the block of data retrieved from said file.

-32-

32. A system according to Claim 21, wherein

2 **the memory further contains cost data associated with different blocks of
data that can be retrieved from said memory; and**

4 **the system further comprises**

6 **means for processing the cost data with said credit signal in response to
a request to retrieve a given said block of data to determine whether retrieval of
said requested block of data is authorized.**

33. A system according to Claim 32, further comprising

2 **means for authenticating said cost data prior to said processing of same.**

34. A system according to Claim 21, wherein

2 **said memory is in a customer data retrieval terminal; and**

4 **the authorization means comprises means for determining in an
authorization center located remotely from said customer terminal whether the
status of an account associated with said customer terminal warrants authorizing
said retrieval, and, if so, providing said encryption key and said credit signal in the
customer data retrieval terminal.**

35. A system according to Claim 34, wherein

2 **the memory further contains cost data associated with different blocks of
data that can be retrieved from said memory; and**

-33-

4 the system further comprises the steps of
6 means for recording in said customer terminal, the cost data for the
blocks of data retrieved in relation to said credit signal provided therein; and
8 means for reporting to the authorization center the record of said cost
data in relation to said credit signal.

36. A system according to Claim 35, futher comprising
2 means for authenticating said report of the record of said cost data in
relation to said credit signal.

37. A system according to Claim 21, wherein the memory is a compact
2 disc ROM.

38. A system for controlling and accounting for retrieval of data from a
2 plurality of identical memories by a corresponding plurality of different data
retrieval terminals, wherein each memory contains an encrypted data file from
4 which retrieval must be authorized, the system comprising

means providing a different unit key in each of the retreival terminals;
6 means for authorizing said retrieval by providing an encryption key
encrypted in the unit key of the given retreival terminal for enabling retrieval of
8 said data in the given retrieval terminal and by providing a credit signal addressed
to the given retrieval terminal for use in limiting the amount of data to be
10 retrieved from said file by the given retrieval terminal;

-34-

means for limiting the amount of data retrieved from said file in the given
12 retrieval terminal in accordance with said credit signal; and

means for recording the amount of data retrieved from said file in said
14 retrieval terminal.

39. A system according to Claim 38, wherein the memory is a compact
2 disc ROM.

40. A system for controlling and accounting for retrieval of data from a
2 memory in a customer data retrieval terminal, wherein the memory contains an
4 encrypted data file from which retrieval must be authorized, the system comprising

6 means for authorizing said retrieval in response to a request to retrieve
8 data from said file in said customer data retrieval terminal by determining in an
4 authorization center located remotely from the customer terminal whether the
status of an account associated with said customer terminal warrants authorizing
6 said retrieval, and, if so, providing in the customer terminal an encryption key for
8 enabling retrieval of data from said file; and

10 means for recording the retrieval of data from said file by said customer
retrieval terminal and debiting said account for said retrieval.

41. A system according to Claim 40, wherein
2 the authorizing means comprise means for encrypting said encryption
key.

-35-

42. A system according to Claim 40, further comprising

2 means for verifying decryption of data pursuant to use of said encryption

key prior to debiting said account.

43. A system according to Claim 40, wherein the memory is a compact

2 disc ROM.

FIG. 1

1/5

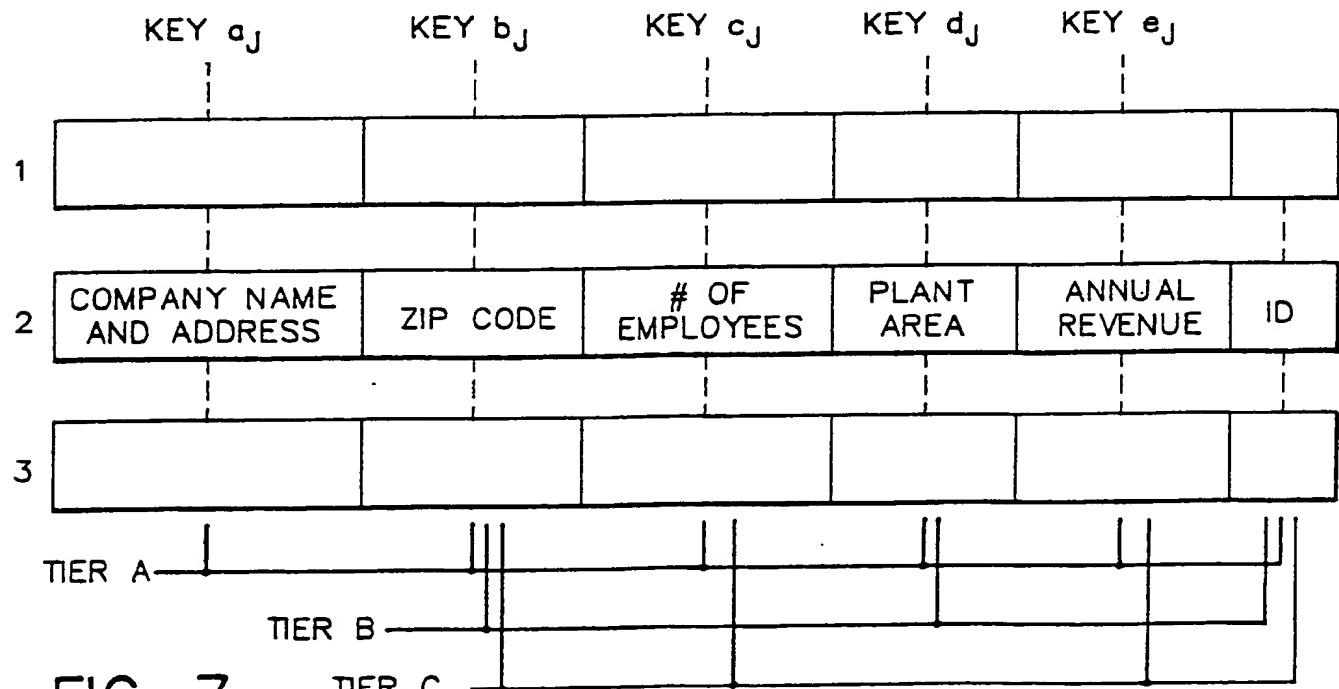
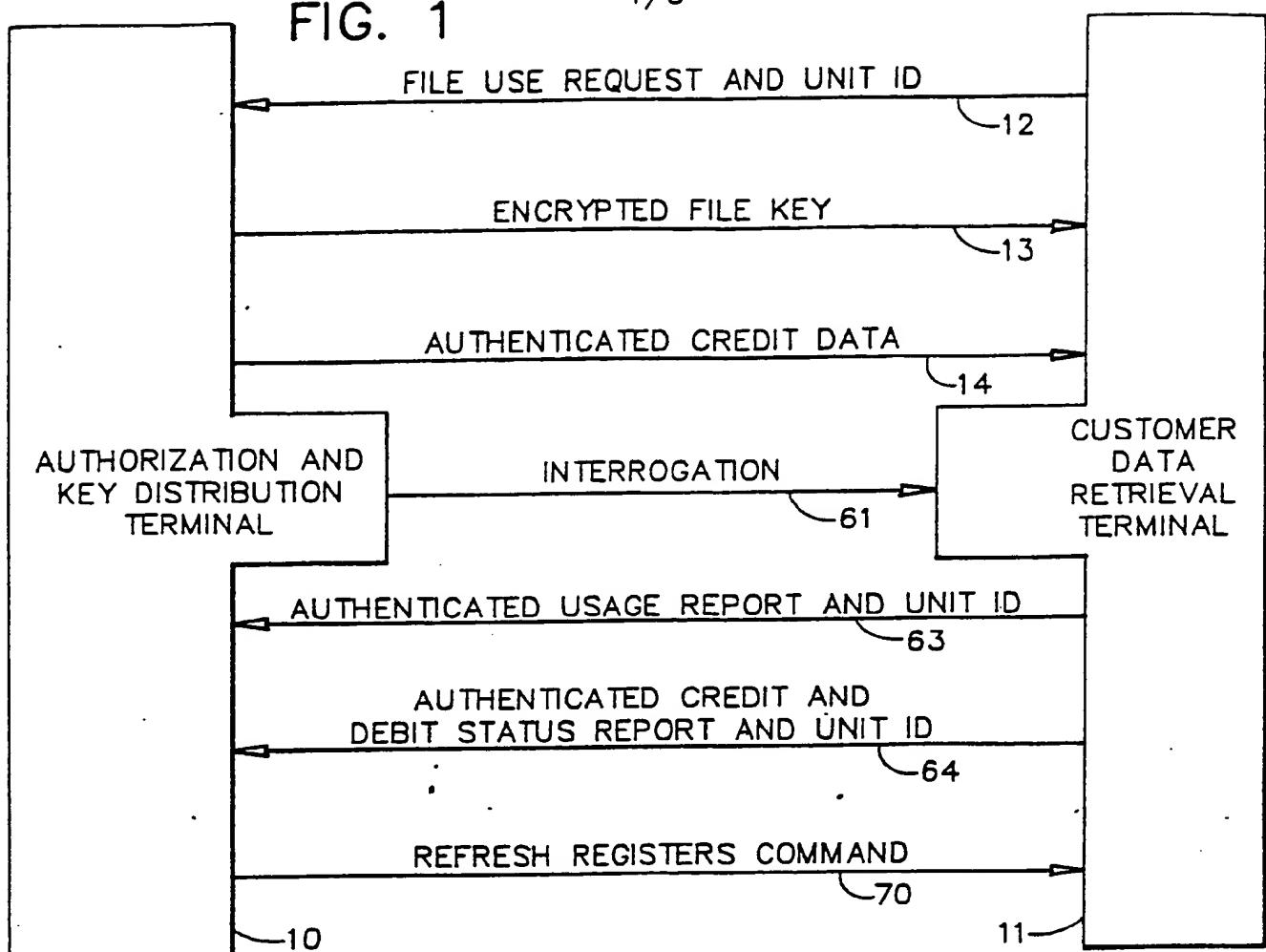
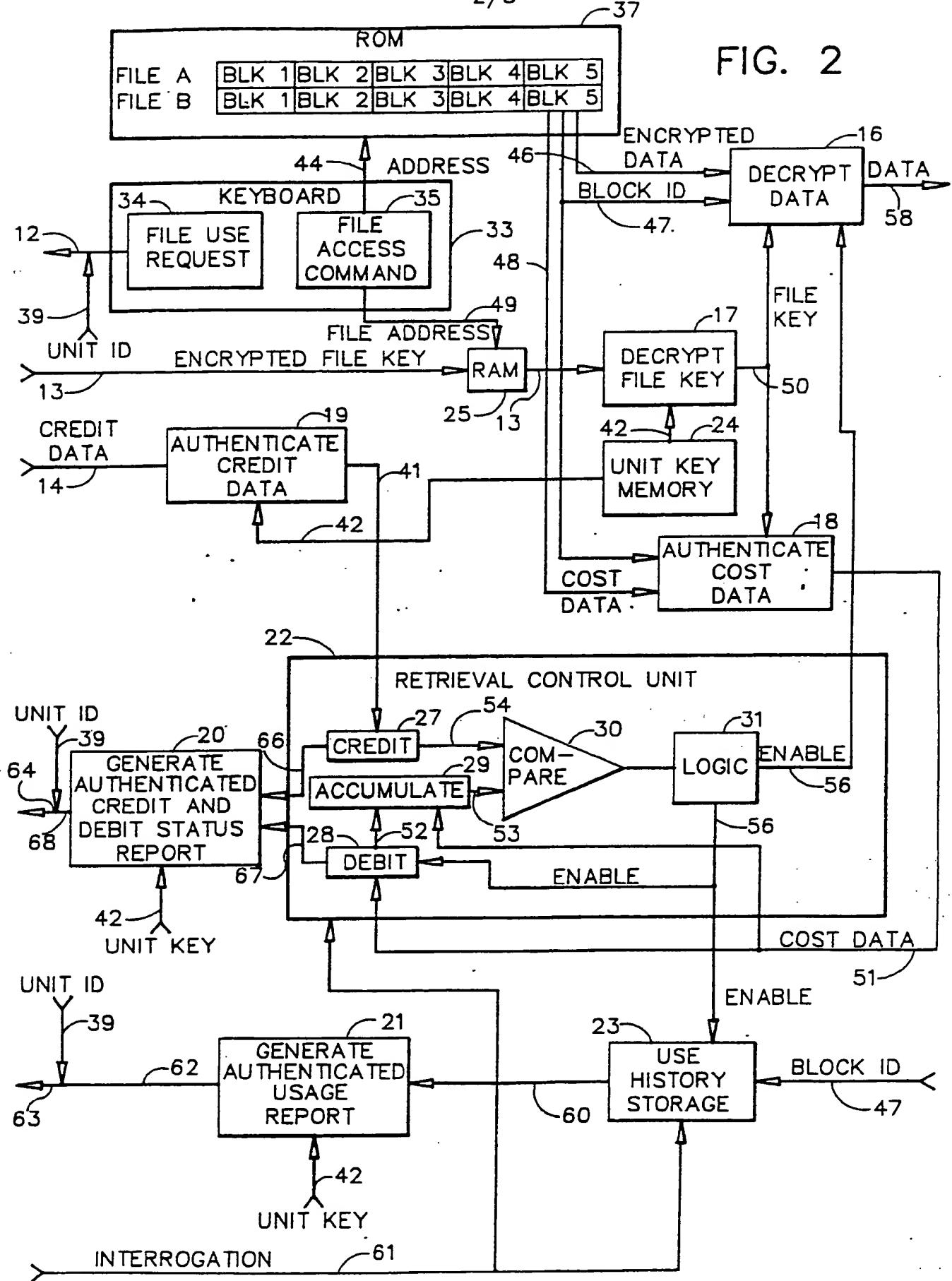


FIG. 7

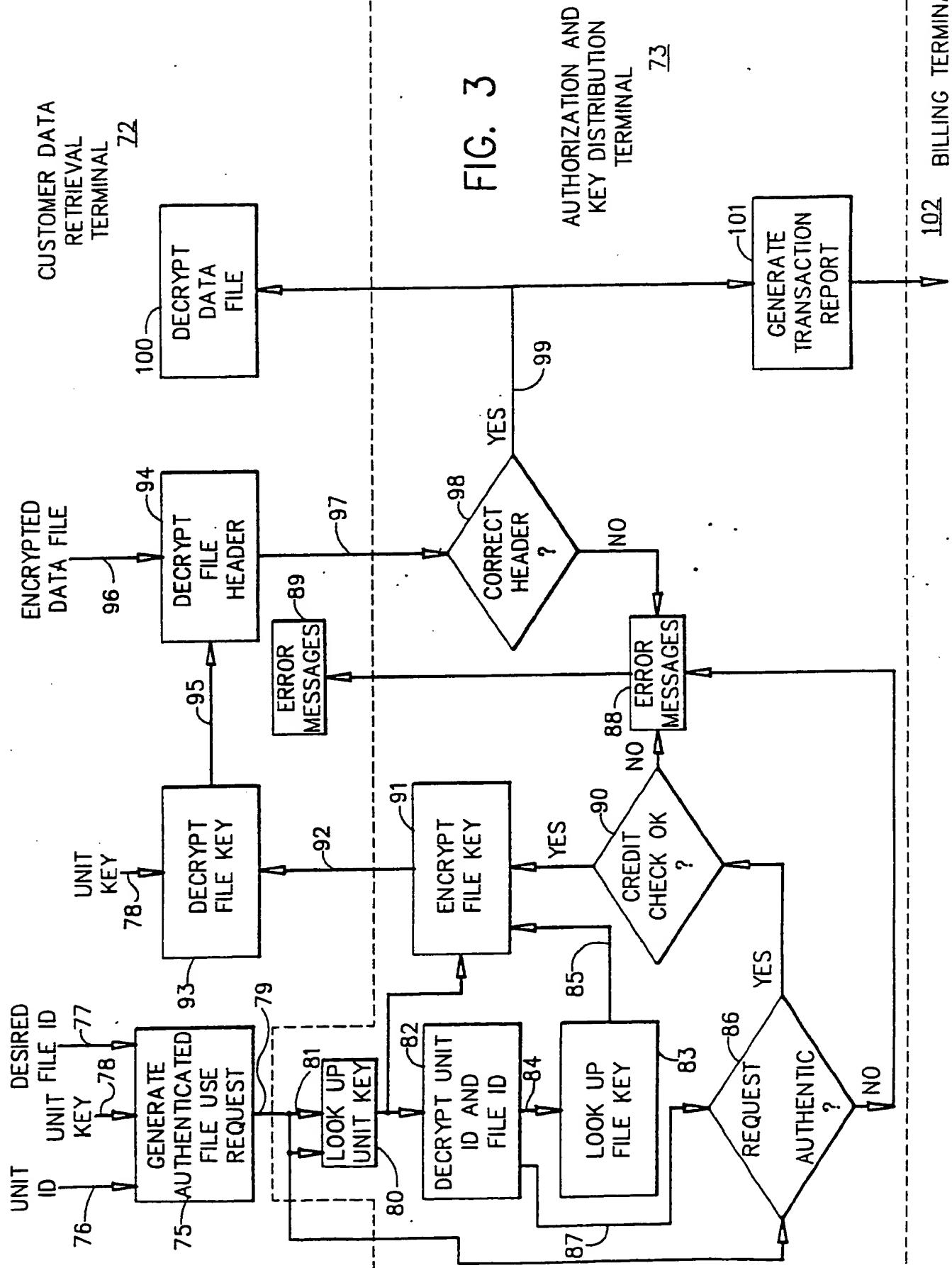
TIER C

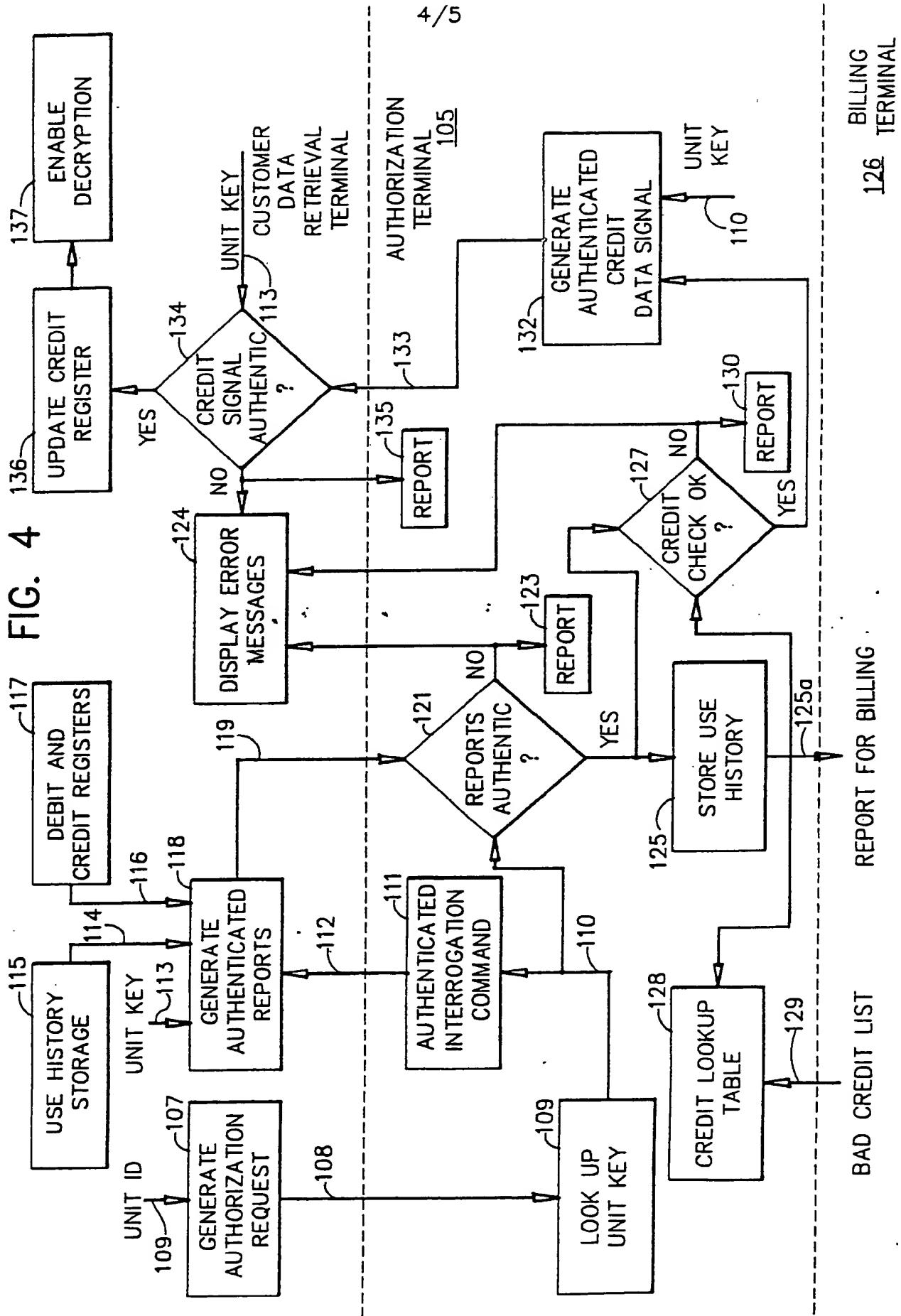
2/5

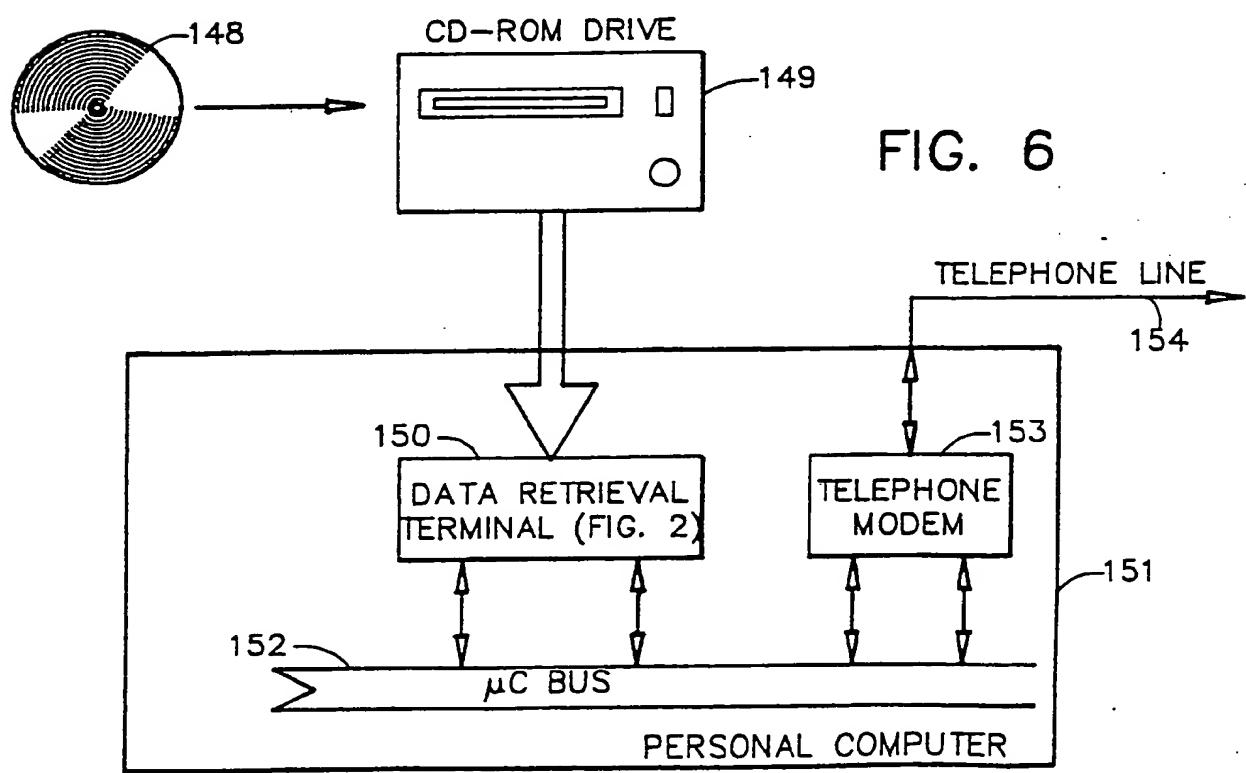
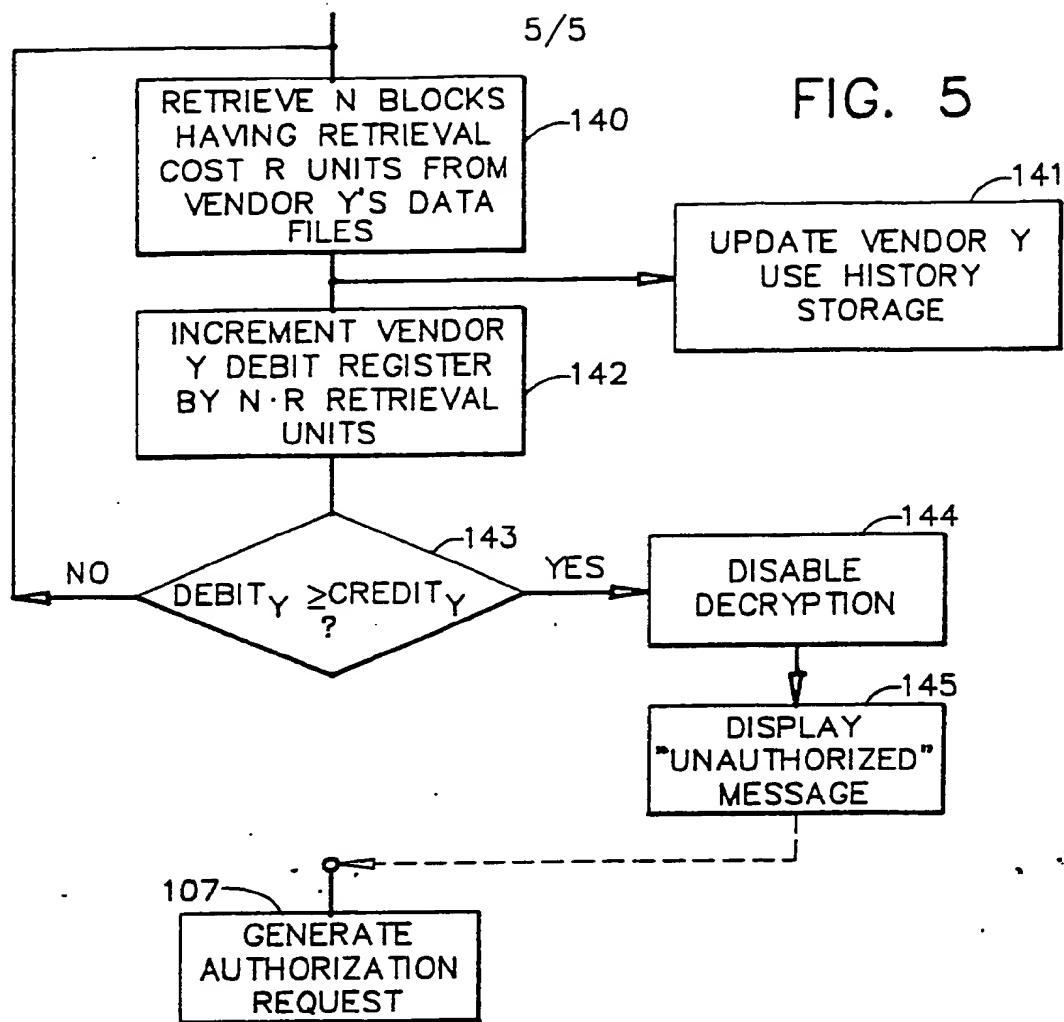


3/5

FIG. 3







INTERNATIONAL SEARCH REPORT

International Application No. PCT/US87/02301

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) ³

According to International Patent Classification (IPC) or to both National Classification and IPC

INT. CL. 4 H04L 9/00

U.S. CL. 380/16, 20, 23-25, 28

II. FIELDS SEARCHED

Minimum Documentation Searched ⁴

Classification System:

Classification Symbols

U.S. CL. 380/16, 20, 23-25, 28

Documentation Searched other than Minimum Documentation
to the Extent that such Documents are Included in the Fields Searched ⁵III. DOCUMENTS CONSIDERED TO BE RELEVANT ⁶

Category ⁷	Citation of Document, ¹⁴ with indication, where appropriate, of the relevant passages ¹⁷	Relevant to Claim No. ¹⁴
Y	US, A. 4,323,921 Published 6 April 1982, Guillou (Fig. #1)	1-43
Y	Computing Surveys 227-249, Vol. 11, No.3. September 1979, 'Data Security', Denning, et al.	1-43

* Special categories of cited documents: ¹⁵

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"Z" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search:

11 November 1987

Date of Mailing of this International Search Report ⁸

23 DEC 1987

International Searching Authority:

ISA/US

Signature of Authorized Officer ⁹*Aaron J. Lewis*
Aaron J. Lewis

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.